

ON A CLASS OF DIAGONAL EQUATIONS OVER FINITE FIELDS

IOULIA N. BAOULINA

To the memory of my first teacher in number theory, Elena B. Gladkova (1953 – 2015)

ABSTRACT. Using properties of Gauss and Jacobi sums, we derive explicit formulas for the number of solutions to a diagonal equation of the form $x_1^{2^m} + \cdots + x_n^{2^m} = 0$ over a finite field of characteristic $p \equiv \pm 3 \pmod{8}$. All of the evaluations are effected in terms of parameters occurring in quadratic partitions of some powers of p .

Keywords: Equation over a finite field; diagonal equation; Gauss sum; Jacobi sum.
Mathematics Subject Classification 2010: 11G25, 11T24

1. INTRODUCTION

Let \mathbb{F}_q be a finite field of characteristic $p > 2$ with $q = p^s$ elements, η be the quadratic character on \mathbb{F}_q ($\eta(x) = +1, -1, 0$ according as x is a square, a non-square or zero in \mathbb{F}_q), and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A diagonal equation over \mathbb{F}_q is an equation of the type

$$a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = b, \quad (1)$$

where $a_1, \dots, a_n \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$ and d_1, \dots, d_n are positive integers. As x_j runs through all elements of \mathbb{F}_q , $x_j^{d_j}$ runs through the same elements as $x_j^{\gcd(d_j, q-1)}$ does with the same multiplicity. Therefore, without loss of generality, we may assume that d_j divides $q-1$ for all j . Denote by $N[a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = b]$ the number of solutions to (1) in \mathbb{F}_q^n .

The pioneering work on diagonal equations has been done by Weil [14], who expressed the number of solutions in terms of Gauss sums. For certain choices of coefficients a_1, \dots, a_n, b , exponents d_1, \dots, d_n and finite fields \mathbb{F}_q , the explicit formulas for the number of solutions can be deduced from Weil's expression, see [3, 4, 6, 8, 10, 11, 12, 13, 15, 16] for some results in this direction. However, in general, it is a difficult task to determine $N[a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = b]$.

In this paper, we consider a diagonal equation of the form

$$x_1^{2^m} + \cdots + x_n^{2^m} = 0, \quad (2)$$

where m is a positive integer with $2^m \mid (q-1)$. It is well known (see [4, Theorem 10.5.1] or [10, Theorems 6.26 and 6.27]) that

$$N[x_1^2 + \cdots + x_n^2 = 0] = \begin{cases} q^{n-1} + \eta((-1)^{n/2})q^{(n-2)/2}(q-1) & \text{if } n \text{ is even,} \\ q^{n-1} & \text{if } n \text{ is odd.} \end{cases}$$

Moreover, if $p \equiv 3 \pmod{4}$ and $2 \mid s$, then it follows from the result of Wolfmann [15, Corollary 4] that

$$N[x_1^4 + \cdots + x_n^4 = 0] = q^{n-1} + (-1)^{((s/2)-1)n} q^{(n-2)/2} (q-1) \cdot \frac{3^n + (-1)^n \cdot 3}{4}.$$

Further, for any m with $2^m \mid (q-1)$, it is not hard to show that

$$N[x_1^{2^m} + x_2^{2^m} = 0] = \begin{cases} 2^m(q-1) + 1 & \text{if } 2^{m+1} \mid (q-1), \\ 1 & \text{if } 2^m \parallel (q-1). \end{cases}$$

The goal of this paper is to determine explicitly $N[x_1^{2^m} + \cdots + x_n^{2^m} = 0]$ for an arbitrary n in the case when $p \equiv \pm 3 \pmod{8}$ and

$$m \geq \begin{cases} 3 & \text{if } p \equiv 3 \pmod{8}, \\ 2 & \text{if } p \equiv -3 \pmod{8}. \end{cases}$$

In Section 3, we treat the case $p \equiv 3 \pmod{8}$. The main results of this section are Theorems 18 and 19, in which we cover the cases $2^{m+1} \mid (q-1)$ and $2^m \parallel (q-1)$, respectively. Our main results in Section 4 are Theorems 22 and 23, in which we deal with the case $p \equiv -3 \pmod{8}$. All of the evaluations in Sections 3 and 4 are effected in terms of parameters occurring in quadratic partitions of some powers of p . The results of numerical experiments are presented in Section 5. Applications of our results to some other diagonal equations are discussed in Section 6.

2. PRELIMINARY LEMMAS

Let, as usual, $\zeta_k = \exp(2\pi i/k)$. Let ψ be a nontrivial character on \mathbb{F}_q . We extend ψ to all of \mathbb{F}_q by setting $\psi(0) = 0$. The Gauss sum $G(\psi)$ over \mathbb{F}_q is defined by

$$G(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x) \zeta_p^{\text{Tr}(x)},$$

where $\text{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{s-1}}$ is the trace of x from \mathbb{F}_q to \mathbb{F}_p . The next lemma gives an expression for $N[a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = 0]$ in terms of Gauss sums.

Lemma 1. *Let $a_1, \dots, a_n \in \mathbb{F}_q^*$, d_1, \dots, d_n be positive integers, d_j divides $q-1$ for all j , and let ψ_j be a character of order d_j on \mathbb{F}_q , $1 \leq j \leq n$. Then*

$$\begin{aligned} N[a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = 0] \\ = q^{n-1} + \frac{q-1}{q} \sum_{\substack{1 \leq j_1 \leq d_1-1 \\ \vdots \\ 1 \leq j_n \leq d_n-1 \\ (j_1/d_1) + \cdots + (j_n/d_n) \in \mathbb{Z}}} \bar{\psi}_1^{j_1}(a_1) \cdots \bar{\psi}_n^{j_n}(a_n) G(\psi_1^{j_1}) \cdots G(\psi_n^{j_n}). \end{aligned}$$

Proof. See [4, Theorems 10.3.1 and 10.4.2] or [10, Equation (6.14)]. \square

We recall some properties of Gauss sums, which will be used throughout this paper.

Lemma 2. *Let ψ be a nontrivial character on \mathbb{F}_q . Then*

- (a) $G(\psi)G(\bar{\psi}) = \psi(-1)q$;
- (b) $G(\psi) = G(\psi^p)$.

Proof. See [4, Theorem 1.1.4(a, d)] or [10, Theorem 5.12(iv,v)]. □

The evaluation of the quadratic Gauss sum $G(\eta)$ is given in the following lemma.

Lemma 3. *We have*

$$G(\eta) = \begin{cases} (-1)^{s-1}q^{1/2} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{s-1}i^s q^{1/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. See [4, Theorem 11.5.4] or [10, Theorem 5.15]. □

The next lemma is a particular case of the Stickelberger theorem.

Lemma 4. *Let $p \equiv 3 \pmod{8}$, $2 \mid s$ and ψ be a biquadratic character on \mathbb{F}_q . Then $G(\psi) = -q^{1/2}$.*

Proof. See [4, Theorem 11.6.3]. □

The following lemma is a special case of the Davenport-Hasse product formula for Gauss sums.

Lemma 5. *Let ψ be a nontrivial character on \mathbb{F}_q with $\psi \neq \eta$. Then*

$$G(\psi)G(\psi\eta) = \bar{\psi}(4)G(\psi^2)G(\eta).$$

Proof. See [4, Theorem 11.3.5] or [10, Corollary 5.29]. □

Let ψ be a nontrivial character on \mathbb{F}_q . The Jacobi sum $J(\psi)$ over \mathbb{F}_q is defined by

$$J(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x)\psi(1-x).$$

An important relationship between Jacobi sums and Gauss sums is presented in the next lemma.

Lemma 6. *Let ψ be a nontrivial character on \mathbb{F}_q with $\psi \neq \eta$. Then*

$$G(\psi)^2 = G(\psi^2)J(\psi).$$

Proof. See [4, Theorem 2.1.3(a)] or [10, Theorem 5.21]. □

Let ψ be a character on \mathbb{F}_q . The lift ψ' of the character ψ from \mathbb{F}_q to the extension field \mathbb{F}_{q^r} is given by

$$\psi'(x) = \psi(N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x)), \quad x \in \mathbb{F}_{q^r},$$

where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{r-1}} = x^{(q^r-1)/(q-1)}$ is the norm of x from \mathbb{F}_{q^r} to \mathbb{F}_q . The basic properties of the lift ψ' of ψ from \mathbb{F}_q to \mathbb{F}_{q^r} are recorded in the next lemma.

Lemma 7. *Let ψ be a character on \mathbb{F}_q and let ψ' denote the lift of ψ from \mathbb{F}_q to \mathbb{F}_{q^r} . Then*

- (a) ψ' is a character on \mathbb{F}_{q^r} ;
- (b) a character λ on \mathbb{F}_{q^r} equals the lift ψ' of some character ψ on \mathbb{F}_q if and only if the order of λ divides $q - 1$;
- (c) ψ' and ψ have the same order.

Proof. See [4, Theorem 11.4.4(a, c, e)]. \square

The following lemma, which is due to Davenport and Hasse, gives the relationship between a Gauss sum and its lift.

Lemma 8. *Let ψ be a nontrivial character on \mathbb{F}_q and let ψ' denote the lift of ψ from \mathbb{F}_q to \mathbb{F}_{q^r} . Then*

$$G(\psi') = (-1)^{r-1} G(\psi)^r.$$

Proof. See [4, Theorem 11.5.2] or [10, Theorem 5.14]. \square

Now we turn to the case $p \equiv \pm 3 \pmod{8}$. The next three lemmas were established in our earlier paper [2] in more general settings (see Lemmas 2.2, 2.13, 2.16, respectively).

Lemma 9. *Let $p \equiv \pm 3 \pmod{8}$, r be an integer, and ξ be a 2^k th primitive root of unity, where $r \geq 3$ and $k \leq r$. Then*

$$\sum_{v=0}^{2^{r-2}-1} \xi^{p^v} = \begin{cases} 2^{r-3}(\xi + \xi^p) & \text{if } k \leq 3, \\ 0 & \text{if } k > 3. \end{cases}$$

Lemma 10. *Let $p \equiv \pm 3 \pmod{8}$ and ψ be a character of order 2^r on \mathbb{F}_q , where*

$$r \geq \begin{cases} 4 & \text{if } p \equiv 3 \pmod{8}, \\ 3 & \text{if } p \equiv -3 \pmod{8}. \end{cases}$$

Then $G(\psi) = G(\psi\eta)$.

Lemma 11. *Let $p \equiv \pm 3 \pmod{8}$ and ψ be a character of order 2^r on \mathbb{F}_q , where $r \geq 3$. Then*

$$\psi(4) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{s/2^{r-2}} & \text{if } p \equiv -3 \pmod{8}. \end{cases}$$

We next relate Gauss sums over \mathbb{F}_q to Jacobi sums over a subfield of \mathbb{F}_q .

Lemma 12. *Let $p \equiv 3 \pmod{8}$ and ψ be a character of order 2^r on \mathbb{F}_q , where $r \geq 3$. Assume that $2^{r+1} \mid (q-1)$. Then $\psi^{2^{r-3}}$ is equal to the lift of some octic character χ on $\mathbb{F}_{p^{s/2^{r-2}}}$. Moreover, $G(\psi) = q^{(2^{r-2}-1)/2^{r-1}} J(\chi)$.*

Proof. We prove the assertion of the lemma by induction on r . Let $16 \mid (q-1)$ and ψ be an octic character on \mathbb{F}_q . As $4 \mid s$, we have $8 \mid (p^{s/2} - 1)$, and Lemma 7 shows that ψ is equal to the lift of some octic character χ on $\mathbb{F}_{p^{s/2}}$, that is, $\chi' = \psi$. Lemmas 6 and 8 yield $G(\psi) = G(\chi') = -G(\chi)^2 = -G(\chi^2)J(\chi)$. Note that χ^2 has order 4. Thus, by Lemma 4, $G(\chi^2) = -q^{1/4}$, and so $G(\psi) = q^{1/4}J(\chi)$. This completes the proof for the case $r = 3$.

Suppose now that $r > 3$, and assume that the result is true when r is replaced by $r - 1$. Let $2^{r+1} \mid (q - 1)$ and ψ be a character of order 2^r on \mathbb{F}_q . Since s is even, we have $\nu_2(q - 1) = \nu_2(p^s - 1) = \nu_2(p^2 - 1) + \nu_2(s) - 1$, where $\nu_2(z)$ denotes the 2-adic valuation of $z \in \mathbb{Z}^+$, i.e., $2^{\nu_2(z)} \parallel z$ (for a proof, see [5, Proposition 1]). Hence $\nu_2(s) = \nu_2(q - 1) - 2 \geq r - 1$. Then $2^{r-2} \mid \frac{s}{2}$, and so $2^r \mid (p^{s/2} - 1)$. By Lemma 7, ψ is equal to the lift of some character ρ of order 2^r on $\mathbb{F}_{p^{s/2}}$, that is $\rho' = \psi$. Applying Lemmas 3, 5, 8, 10, 11 and using the fact that $8 \mid s$, we deduce

$$\begin{aligned} G(\psi) &= G(\rho') = -G(\rho)^2 = -G(\rho)G(\rho\eta_0) = -G(\rho^2)G(\eta_0) \\ &= -(-1)^{(s/2)-1} i^{s/2} p^{s/4} G(\rho^2) = q^{1/4} G(\rho^2), \end{aligned} \quad (3)$$

where η_0 denotes the quadratic character on $\mathbb{F}_{p^{s/2}}$. Note that ρ^2 has order 2^{r-1} and $2^r \mid (p^{s/2} - 1)$. Hence, by inductive hypothesis, $(\rho^2)^{2^{r-4}} = \rho^{2^{r-3}}$ is equal to the lift of some octic character χ on $\mathbb{F}_{p^{(s/2)/2^{r-3}}} = \mathbb{F}_{p^{s/2^{r-2}}}$ and $G(\rho^2) = (p^{s/2})^{(2^{r-3}-1)/2^{r-2}} J(\chi) = q^{(2^{r-3}-1)/2^{r-1}} J(\chi)$. Substituting this expression for $G(\rho^2)$ into (3), we obtain $G(\psi) = q^{(2^{r-2}-1)/2^{r-1}} J(\chi)$. It remains to show that $\psi^{2^{r-3}}$ is equal to the lift of χ . Indeed, for any $x \in \mathbb{F}_q$ we have

$$\begin{aligned} \chi(N_{\mathbb{F}_q/\mathbb{F}_{p^{s/2^{r-2}}}}(x)) &= \chi(x^{(p^s-1)/(p^{s/2^{r-2}}-1)}) = \chi((x^{(p^s-1)/(p^{s/2}-1)})^{(p^{s/2}-1)/(p^{s/2^{r-2}}-1)}) \\ &= \chi(N_{\mathbb{F}_{p^{s/2}}/\mathbb{F}_{p^{s/2^{r-2}}}}(x^{(p^s-1)/(p^{s/2}-1)})) = \rho^{2^{r-3}}(x^{(p^s-1)/(p^{s/2}-1)}) \\ &= \left(\rho(N_{\mathbb{F}_{p^s}/\mathbb{F}_{p^{s/2}}}(x)) \right)^{2^{r-3}} = \psi^{2^{r-3}}(x). \end{aligned}$$

Therefore $\chi' = \psi^{2^{r-3}}$, and the result now follows by the principle of mathematical induction. \square

For the case $p \equiv -3 \pmod{8}$ a similar result is given in the next lemma.

Lemma 13. *Let $p \equiv -3 \pmod{8}$ and ψ be a character of order 2^r on \mathbb{F}_q , where $r \geq 2$. Assume that $2^{r+1} \mid (q - 1)$. Then $\psi^{2^{r-2}}$ is equal to the lift of some biquadratic character χ on $\mathbb{F}_{p^{s/2^{r-1}}}$. Moreover, $G(\psi) = (-1)^{s(r-1)/2^{r-1}} q^{(2^{r-1}-1)/2^r} J(\chi)$.*

Proof. The proof is analogous to that of Lemma 12. \square

From now on we shall assume that $p \equiv \pm 3 \pmod{8}$, $2^m \mid (q - 1)$, λ is a fixed character of order 2^m on \mathbb{F}_q and

$$m \geq \begin{cases} 3 & \text{if } p \equiv 3 \pmod{8}, \\ 2 & \text{if } p \equiv -3 \pmod{8}. \end{cases}$$

We observe that $2^{m-2} \mid s$. To simplify notation, put $N = N[x_1^{2^m} + \dots + x_n^{2^m} = 0]$. Employing Lemma 1, we obtain

$$\begin{aligned} N &= q^{n-1} + \frac{q-1}{q} \sum_{\substack{1 \leq j_1, \dots, j_n \leq 2^m-1 \\ j_1 + \dots + j_n \equiv 0 \pmod{2^m}}} G(\lambda^{j_1}) \dots G(\lambda^{j_n}) \\ &= q^{n-1} + \frac{q-1}{2^m q} \sum_{c=1}^{2^m} \left(\sum_{j=1}^{2^m-1} G(\lambda^j) \zeta_{2^m}^{cj} \right)^n. \end{aligned} \quad (4)$$

For $t = 0, 1, \dots, m$, set

$$S_t = \sum_{\substack{c=1 \\ 2^t \parallel c}}^{2^m} \left(\sum_{j=1}^{2^m-1} G(\lambda^j) \zeta_{2^m}^{cj} \right)^n = \sum_{\substack{c_0=1 \\ 2^t \nmid c_0}}^{2^{m-t}} \left(\sum_{j=1}^{2^m-1} G(\lambda^j) \zeta_{2^{m-t}}^{c_0 j} \right)^n.$$

Then (4) can be rewritten in the form

$$N = q^{n-1} + \frac{q-1}{2^m q} \sum_{t=0}^m S_t. \quad (5)$$

For $r = 1, 2, \dots, m$ and any odd integer c_0 , set

$$W_{r,t}(c_0) = \sum_{\substack{j=1 \\ 2^{m-r} \parallel j}}^{2^m-1} G(\lambda^j) \zeta_{2^{m-t}}^{c_0 j} = \sum_{\substack{j_0=1 \\ 2^t \nmid j_0}}^{2^r-1} G(\lambda^{2^{m-r} j_0}) \zeta_{2^{m-t}}^{2^{m-r} c_0 j_0}.$$

In this notation we can write

$$S_t = \sum_{\substack{c_0=1 \\ 2^t \nmid c_0}}^{2^{m-t}} \left(\sum_{r=1}^m W_{r,t}(c_0) \right)^n. \quad (6)$$

Lemma 14. *We have*

$$\begin{aligned} W_{1,t}(c_0) &= \begin{cases} -G(\eta) & \text{if } t = 0, \\ G(\eta) & \text{if } t \geq 1, \end{cases} \\ W_{2,t}(c_0) &= \begin{cases} G(\lambda^{2^{m-2}}) + G(\bar{\lambda}^{2^{m-2}}) & \text{if } t \geq 2, \\ -(G(\lambda^{2^{m-2}}) + G(\bar{\lambda}^{2^{m-2}})) & \text{if } t = 1, \\ i^{c_0} (G(\lambda^{2^{m-2}}) - G(\bar{\lambda}^{2^{m-2}})) & \text{if } t = 0, \end{cases} \end{aligned}$$

and, for $3 \leq r \leq m$,

$$W_{r,t}(c_0) = \begin{cases} 2^{r-2}(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}})) & \text{if } r \leq t, \\ -2^{r-2}(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}})) & \text{if } r = t+1, \\ 2^{r-2}i^{c_0}(G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}})) & \text{if } r = t+2 \text{ and } p \equiv -3 \pmod{8}, \\ 2^{r-3}i\sqrt{2}(G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}})) & \text{if } r = t+3, p \equiv 3 \pmod{8} \\ & \text{and } c_0 \equiv 1 \text{ or } 3 \pmod{8}, \\ -2^{r-3}i\sqrt{2}(G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}})) & \text{if } r = t+3, p \equiv 3 \pmod{8} \\ & \text{and } c_0 \equiv 5 \text{ or } 7 \pmod{8}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We first observe that

$$\begin{aligned} W_{1,t}(c_0) &= G(\lambda^{2^{m-1}})\zeta_{2^{m-t}}^{2^{m-1}c_0} = G(\eta)\zeta_{2^{m-t}}^{2^{m-1}c_0} = \begin{cases} -G(\eta) & \text{if } t = 0, \\ G(\eta) & \text{if } t \geq 1, \end{cases} \\ W_{2,t}(c_0) &= G(\lambda^{2^{m-2}})\zeta_{2^{m-t}}^{2^{m-2}c_0} + G(\lambda^{3 \cdot 2^{m-2}})\zeta_{2^{m-t}}^{3 \cdot 2^{m-2}c_0} \\ &= \begin{cases} G(\lambda^{2^{m-2}}) + G(\bar{\lambda}^{2^{m-2}}) & \text{if } t \geq 2, \\ -(G(\lambda^{2^{m-2}}) + G(\bar{\lambda}^{2^{m-2}})) & \text{if } t = 1, \\ i^{c_0}(G(\lambda^{2^{m-2}}) - G(\bar{\lambda}^{2^{m-2}})) & \text{if } t = 0. \end{cases} \end{aligned}$$

Now assume that $3 \leq r \leq m$. Since $\lambda^{2^{m-r}}$ has order 2^r and $\pm p^0, \pm p^1, \dots, \pm p^{2^{r-2}-1}$ is a reduced residue system modulo 2^r , we conclude that

$$W_{r,t}(c_0) = \sum_{u \in \{\pm 1\}} \sum_{v=0}^{2^{r-2}-1} G(\lambda^{2^{m-r}up^v})\zeta_{2^{m-t}}^{2^{m-r}c_0up^v}.$$

Applying Lemma 2(b), we obtain

$$W_{r,t}(c_0) = G(\lambda^{2^{m-r}}) \sum_{v=0}^{2^{r-2}-1} \zeta_{2^{m-t}}^{2^{m-r}c_0p^v} + G(\bar{\lambda}^{2^{m-r}}) \sum_{v=0}^{2^{r-2}-1} \bar{\zeta}_{2^{m-t}}^{2^{m-r}c_0p^v}. \quad (7)$$

If $r \leq t$, then $\zeta_{2^{m-t}}^{2^{m-r}c_0} = \bar{\zeta}_{2^{m-t}}^{2^{m-r}c_0} = 1$ and $W_{r,t}(c_0) = 2^{r-2}(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}))$. Suppose that $r > t$. Then $\zeta_{2^{m-t}}^{2^{m-r}c_0} = \zeta_{2^{r-t}}^{c_0}$ is a 2^{r-t} th primitive root of unity. If $r = t+1$, then $\zeta_{2^{r-t}}^{c_0} = -1$, and so $W_{r,t}(c_0) = -2^{r-2}(G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}))$. If $r = t+2$, then $\zeta_{2^{r-t}}^{c_0} = i^{c_0}$. Appealing to Lemma 9, we deduce that

$$\sum_{v=0}^{2^{r-2}-1} \zeta_{2^{m-t}}^{2^{m-r}c_0p^v} = \sum_{v=0}^{2^{r-2}-1} i^{c_0p^v} = 2^{r-3}(i^{c_0} + i^{c_0p}) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod{8}, \\ 2^{r-2}i^{c_0} & \text{if } p \equiv -3 \pmod{8}, \end{cases}$$

and the result follows from (7). Next assume that $r = t + 3$. Again by Lemma 9,

$$\begin{aligned} \sum_{v=0}^{2^{r-2}-1} \zeta_{2^{m-t}}^{2^{m-r}c_0p^v} &= \sum_{v=0}^{2^{r-2}-1} \zeta_8^{c_0p^v} = 2^{r-3}(\zeta_8^{c_0} + \zeta_8^{c_0p}) \\ &= \begin{cases} 2^{r-3}i\sqrt{2} & \text{if } p \equiv 3 \pmod{8} \text{ and } c_0 \equiv 1 \text{ or } 3 \pmod{8}, \\ -2^{r-3}i\sqrt{2} & \text{if } p \equiv 3 \pmod{8} \text{ and } c_0 \equiv 5 \text{ or } 7 \pmod{8}, \\ 0 & \text{if } p \equiv -3 \pmod{8}. \end{cases} \end{aligned}$$

The result now follows from (7) and the fact that $\bar{\zeta}_8^{c_0} + \bar{\zeta}_8^{3c_0} = -(\zeta_8^{c_0} + \zeta_8^{3c_0})$. Finally, assume that $r > t + 3$. In view of Lemma 9,

$$\sum_{v=0}^{2^{r-2}-1} \zeta_{2^{m-t}}^{2^{m-r}c_0p^v} = \sum_{v=0}^{2^{r-2}-1} \zeta_{2^{r-t}}^{c_0p^v} = 0,$$

and (7) yields $W_{r,t}(c_0) = 0$. This completes the proof of Lemma 14. \square

From Lemma 14 we see that $W_{r,m-1}(1) = W_{r,m}(1)$ for $1 \leq r \leq m-1$, and $W_{m,m-1}(1) = -W_{m,m}(1)$. Note also that in the case $p \equiv 3 \pmod{8}$ we have $G(\lambda^{2^{m-2}}) = G(\bar{\lambda}^{2^{m-2}}) = -q^{1/2}$ by Lemma 4. Hence in this case $W_{2,0}(c_0) = 0$ for any odd c_0 . In view of these observations, the following corollary is an immediate consequence of Lemma 14.

Corollary 15. *We have*

$$S_{m-1} + S_m = \left(\sum_{r=1}^{m-1} W_{r,m}(1) + W_{m,m}(1) \right)^n + \left(\sum_{r=1}^{m-1} W_{r,m}(1) - W_{m,m}(1) \right)^n.$$

Furthermore, if $p \equiv 3 \pmod{8}$, then

$$S_{m-2} = 2 \cdot \left(\sum_{r=1}^{m-1} W_{r,m-2}(1) \right)^n,$$

and, for $t \leq m-3$,

$$S_t = 2^{m-t-2} \left[\left(\sum_{r=1}^{t+1} W_{r,t}(1) + W_{t+3,t}(1) \right)^n + \left(\sum_{r=1}^{t+1} W_{r,t}(1) - W_{t+3,t}(1) \right)^n \right].$$

If $p \equiv -3 \pmod{8}$ and $t \leq m-2$, then

$$S_t = 2^{m-t-2} \left[\left(\sum_{r=1}^{t+1} W_{r,t}(1) + W_{t+2,t}(1) \right)^n + \left(\sum_{r=1}^{t+1} W_{r,t}(1) - W_{t+2,t}(1) \right)^n \right].$$

3. THE CASE $p \equiv 3 \pmod{8}$

In this section, let $p \equiv 3 \pmod{8}$, $q = p^s \equiv 1 \pmod{2^m}$, $m \geq 3$. As before, λ is a fixed character of order 2^m on \mathbb{F}_q .

For $r = 2, 3, \dots, m$, define the integers A_r and B_r by

$$p^{s/2^{r-2}} = A_r^2 + 2B_r^2, \quad A_r \equiv -1 \pmod{4}, \quad p \nmid A_r. \quad (8)$$

It is well known [4, Lemma 3.0.1] that for each fixed r , (8) determines A_r uniquely but determines B_r only up to sign. Also, if $2^{r-1} \mid s$, or, equivalently, $2^{r+1} \mid (q-1)$, and χ is an octic character on $\mathbb{F}_{p^{s/2^{r-2}}}$ then $J(\chi) = A_r \pm |B_r| i \sqrt{2}$ (see [1, Lemma 17]). Combining this last fact with Lemma 12, we deduce the following result.

Lemma 16. *Let r be an integer with $3 \leq r \leq m$ and assume that $2^{r+1} \mid (q-1)$. Then*

$$G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) = 2A_r q^{(2^{r-2}-1)/2^{r-1}}$$

and

$$G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}}) = \pm 2|B_r| q^{(2^{r-2}-1)/2^{r-1}} i \sqrt{2}.$$

Lemma 16 allows us to evaluate $G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}})$ and $G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}})$ (in the latter case only up to sign) if either $3 \leq r \leq m-1$ or $r = m$ and $2^{m+1} \mid (q-1)$. For the remaining case $r = m$ and $2^m \parallel (q-1)$, we need the following lemma.

Lemma 17. *Assume that $2^m \parallel (q-1)$. Then*

$$G(\lambda) + G(\bar{\lambda}) = \pm 2A_m q^{(2^{m-2}-1)/2^{m-1}} i$$

and

$$G(\lambda) - G(\bar{\lambda}) = \pm 2|B_m| q^{(2^{m-2}-1)/2^{m-1}} \sqrt{2}.$$

Proof. Since $2^m \parallel (q-1)$, it follows from Lemma 2(a) that

$$(G(\lambda) + G(\bar{\lambda}))^2 = G(\lambda)^2 + G(\bar{\lambda})^2 + 2\lambda(-1)q = G(\lambda)^2 + G(\bar{\lambda})^2 - 2q.$$

If $m = 3$, then, by Lemmas 4 and 6,

$$G(\lambda)^2 + G(\bar{\lambda})^2 = G(\lambda^2)J(\lambda) + G(\bar{\lambda}^2)J(\bar{\lambda}) = -2A_2 q^{1/2}.$$

If $m \geq 4$, then Lemmas 3, 5, 10, 11 and 16 yield

$$\begin{aligned} G(\lambda)^2 + G(\bar{\lambda})^2 &= G(\lambda)G(\lambda\eta) + G(\bar{\lambda})G(\bar{\lambda}\eta) = \bar{\lambda}(4)G(\lambda^2)G(\eta) + \lambda(4)G(\bar{\lambda}^2)G(\eta) \\ &= -q^{1/2}(G(\lambda^2) + G(\bar{\lambda}^2)) = -2A_{m-1} q^{(2^{m-2}-1)/2^{m-2}}. \end{aligned}$$

Thus, in both cases,

$$(G(\lambda) + G(\bar{\lambda}))^2 = -2q^{(2^{m-2}-1)/2^{m-2}} (A_{m-1} + p^{s/2^{m-2}}). \quad (9)$$

Note that

$$A_{m-1}^2 + 2B_{m-1}^2 = p^{s/2^{m-3}} = (p^{s/2^{m-2}})^2 = (A_m^2 + 2B_m^2)^2 = (A_m^2 - 2B_m^2)^2 + 2 \cdot (2A_m B_m)^2.$$

Hence $A_{m-1} = \pm(A_m^2 - 2B_m^2)$. Since $p^{s/2^{m-2}} = A_m^2 + 2B_m^2 \equiv 3 \pmod{8}$, B_m is odd, and so $A_{m-1} = A_m^2 - 2B_m^2$. Substituting the expressions for $p^{s/2^{m-2}}$ and

A_{m-1} into (9) and taking square roots of both sides, we find that $G(\lambda) + G(\bar{\lambda}) = \pm 2A_m q^{(2^{m-2}-1)/2^{m-1}} i$. Similarly,

$$(G(\lambda) - G(\bar{\lambda}))^2 = -2q^{(2^{m-2}-1)/2^{m-2}} (A_{m-1} - p^{s/2^{m-2}}) = 8B_m^2 q^{(2^{m-2}-1)/2^{m-2}},$$

which implies that $G(\lambda) - G(\bar{\lambda}) = \pm 2|B_m| q^{(2^{m-2}-1)/2^{m-1}} \sqrt{2}$. \square

We are now ready to determine the number N of solutions to (2) in the case $p \equiv 3 \pmod{8}$. In the proofs of the next two theorems, we shall frequently employ Lemmas 14–17 and Corollary 15 without further comments.

Theorem 18. *Let $p \equiv 3 \pmod{8}$ and $2^{m+1} \mid (q-1)$. If $m = 3$ then*

$$N = q^{n-1} + \frac{q-1}{8q} \left[2 \cdot \left((q^{\frac{1}{2}} + 4B_3 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 4B_3 q^{\frac{1}{4}})^n \right) + 2q^{\frac{n}{2}} \right. \\ \left. + \left(-3q^{\frac{1}{2}} + 4A_3 q^{\frac{1}{4}} \right)^n + \left(-3q^{\frac{1}{2}} - 4A_3 q^{\frac{1}{4}} \right)^n \right].$$

If $m \geq 4$ then

$$N = q^{n-1} + \frac{q-1}{2^m q} \cdot \left[2^{m-2} \cdot \left((q^{\frac{1}{2}} + 4B_3 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 4B_3 q^{\frac{1}{4}})^n \right) \right. \\ \left. + 2^{m-3} \cdot \left((q^{\frac{1}{2}} + 8B_4 q^{\frac{3}{8}})^n + (q^{\frac{1}{2}} - 8B_4 q^{\frac{3}{8}})^n \right) \right. \\ \left. + \sum_{t=2}^{m-3} 2^{m-t-2} \left((-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} + 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right. \right. \\ \left. \left. + (-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} - 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right) \right. \\ \left. + 2 \cdot \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^n \right. \\ \left. + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^n \right. \\ \left. + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^m 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \right)^n \right].$$

The integers A_r and $|B_r|$ are uniquely determined by (8).

Proof. Since $2^{m+1} \mid (q-1)$, $m \geq 3$ and $\lambda^{2^{m-2}}$ has order four, we see that

$$W_{1,m}(1) = -q^{1/2}, \quad W_{2,m}(1) = -2q^{1/2}, \\ W_{r,m}(1) = 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, \quad 3 \leq r \leq m.$$

Hence

$$\begin{aligned} S_{m-1} + S_m &= \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} \right)^n \\ &\quad + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^m 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} \right)^n. \end{aligned} \quad (10)$$

Next,

$$\begin{aligned} W_{1,m-2}(1) &= -q^{1/2}, & W_{2,m-2}(1) &= \begin{cases} 2q^{1/2} & \text{if } m = 3, \\ -2q^{1/2} & \text{if } m \geq 4, \end{cases} \\ W_{r,m-2}(1) &= 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, & 3 \leq r \leq m-2, & \quad m \geq 5, \\ W_{m-1,m-2}(1) &= -2^{m-2} A_{m-1} q^{(2^{m-3}-1)/2^{m-2}}, & m \geq 4. \end{aligned}$$

Thus

$$S_{m-2} = \begin{cases} 2q^{\frac{n}{2}} & \text{if } m = 3, \\ 2 \cdot \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^n & \text{if } m \geq 4. \end{cases} \quad (11)$$

Now assume that $2 \leq t \leq m-3$, $m \geq 5$. Then

$$\begin{aligned} W_{1,t}(1) &= -q^{1/2}, & W_{2,t}(1) &= -2q^{1/2}, \\ W_{r,t}(1) &= 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, & 3 \leq r \leq t, & \quad t \geq 3, \\ W_{t+1,t}(1) &= -2^t A_{t+1} q^{(2^{t-1}-1)/2^t}, & W_{t+3,t}(1) &= \pm 2^{t+2} |B_{t+3}| q^{(2^{t+1}-1)/2^{t+2}}. \end{aligned}$$

Therefore,

$$\begin{aligned} S_t &= 2^{m-t-2} \left(\left(-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} + 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right)^n \right. \\ &\quad \left. + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} - 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}} \right)^n \right). \end{aligned} \quad (12)$$

If $m \geq 4$, then

$$W_{1,1}(1) = -q^{1/2}, \quad W_{2,1}(1) = 2q^{1/2}, \quad W_{4,1}(1) = \pm 8 |B_4| q^{3/8}.$$

This yields

$$S_1 = 2^{m-3} \cdot \left((q^{\frac{1}{2}} + 8B_4 q^{\frac{3}{8}})^n + (q^{\frac{1}{2}} - 8B_4 q^{\frac{3}{8}})^n \right). \quad (13)$$

Finally, we have

$$W_{1,0}(1) = q^{1/2}, \quad W_{3,0}(1) = \pm 4 |B_3| q^{1/4},$$

and so

$$S_0 = 2^{m-2} \cdot \left((q^{\frac{1}{2}} + 4B_3 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 4B_3 q^{\frac{1}{4}})^n \right). \quad (14)$$

Substituting (10)–(14) into (5), we obtain the asserted result. \square

Theorem 19. *Let $p \equiv 3 \pmod{8}$ and $2^m \parallel (q-1)$. If $m = 3$ then*

$$N = q^{n-1} + \frac{q-1}{8q} \left[2 \cdot \left((-q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}}i)^n + (-q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}}i)^n \right) + 2 \cdot 3^n q^{\frac{n}{2}} \right. \\ \left. + \left(-q^{\frac{1}{2}} + 4A_3q^{\frac{1}{4}}i \right)^n + \left(-q^{\frac{1}{2}} - 4A_3q^{\frac{1}{4}}i \right)^n \right].$$

If $m = 4$ then

$$N = q^{n-1} + \frac{q-1}{16q} \left[4 \cdot \left((q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}})^n \right) \right. \\ \left. + 2 \cdot \left((q^{\frac{1}{2}} + 8B_4q^{\frac{3}{8}}i)^n + (q^{\frac{1}{2}} - 8B_4q^{\frac{3}{8}}i)^n \right) + 2 \cdot \left(-3q^{\frac{1}{2}} - 4A_3q^{\frac{1}{4}} \right)^n \right. \\ \left. + \left(-3q^{\frac{1}{2}} + 4A_3q^{\frac{1}{4}} + 8A_4q^{\frac{3}{8}}i \right)^n + \left(-3q^{\frac{1}{2}} + 4A_3q^{\frac{1}{4}} - 8A_4q^{\frac{3}{8}}i \right)^n \right].$$

If $m \geq 5$ then

$$N = q^{n-1} + \frac{q-1}{2^m q} \left[2^{m-2} \cdot \left((q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}})^n \right) \right. \\ \left. + 2^{m-3} \cdot \left((q^{\frac{1}{2}} + 8B_4q^{\frac{3}{8}})^n + (q^{\frac{1}{2}} - 8B_4q^{\frac{3}{8}})^n \right) \right. \\ \left. + \sum_{t=2}^{m-4} 2^{m-t-2} \left((-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} + 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right. \right. \\ \left. \left. + (-3q^{\frac{1}{2}} + \sum_{r=3}^t 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^t A_{t+1} q^{\frac{2^{t-1}-1}{2^t}} - 2^{t+2} B_{t+3} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right) \right. \\ \left. + 2 \cdot \left((-3q^{\frac{1}{2}} + \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} + 2^{m-1} B_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i)^n \right. \right. \\ \left. \left. + (-3q^{\frac{1}{2}} + \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} - 2^{m-1} B_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i)^n \right) \right. \\ \left. + 2 \cdot \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} \right)^n \right. \\ \left. + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i \right)^n \right. \\ \left. + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i \right)^n \right].$$

The integers A_r and $|B_r|$ are uniquely determined by (8).

Proof. Since $2^m \parallel (q-1)$, we find that

$$\begin{aligned} W_{1,m}(1) &= \begin{cases} q^{1/2} & \text{if } m = 3, \\ -q^{1/2} & \text{if } m \geq 4, \end{cases} & W_{2,m}(1) &= -2q^{1/2}, \\ W_{r,m}(1) &= 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, & 3 \leq r \leq m-1, & \quad m \geq 4, \\ W_{m,m}(1) &= \pm 2^{m-1} A_m q^{(2^{m-2}-1)/2^{m-1}} i. \end{aligned}$$

This yields

$$S_{m-1} + S_m = \left(-q^{\frac{1}{2}} + 4A_3 q^{\frac{1}{4}} i\right)^n + \left(-q^{\frac{1}{2}} - 4A_3 q^{\frac{1}{4}} i\right)^n \quad (15)$$

if $m = 3$, and

$$\begin{aligned} S_{m-1} + S_m &= \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} + 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i\right)^n \\ &\quad + \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-1} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-1} A_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i\right)^n \end{aligned} \quad (16)$$

if $m \geq 4$. Furthermore,

$$\begin{aligned} W_{1,m-2}(1) &= \begin{cases} q^{1/2} & \text{if } m = 3, \\ -q^{1/2} & \text{if } m \geq 4, \end{cases} & W_{2,m-2}(1) &= \begin{cases} 2q^{1/2} & \text{if } m = 3, \\ -2q^{1/2} & \text{if } m \geq 4, \end{cases} \\ W_{r,m-2}(1) &= 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, & 3 \leq r \leq m-2, & \quad m \geq 5, \\ W_{m-1,m-2}(1) &= -2^{m-2} A_{m-1} q^{(2^{m-3}-1)/2^{m-2}}, & m \geq 4. \end{aligned}$$

Hence

$$S_{m-2} = \begin{cases} 2 \cdot 3^n q^{\frac{n}{2}} & \text{if } m = 3, \\ 2 \cdot \left(-3q^{\frac{1}{2}} + \sum_{r=3}^{m-2} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-2} A_{m-1} q^{\frac{2^{m-3}-1}{2^{m-2}}} i\right)^n & \text{if } m \geq 4. \end{cases} \quad (17)$$

If $m \geq 4$, then

$$\begin{aligned} W_{1,m-3}(1) &= -q^{1/2}, & W_{2,m-3}(1) &= \begin{cases} 2q^{1/2} & \text{if } m = 4, \\ -2q^{1/2} & \text{if } m \geq 5, \end{cases} \\ W_{r,m-3}(1) &= 2^{r-1} A_r q^{(2^{r-2}-1)/2^{r-1}}, & 3 \leq r \leq m-3, & \quad m \geq 6, \\ W_{m-2,m-3}(1) &= -2^{m-3} A_{m-2} q^{(2^{m-4}-1)/2^{m-3}}, & m \geq 5, \\ W_{m,m-3}(1) &= \pm 2^{m-1} |B_m| q^{(2^{m-2}-1)/2^{m-1}} i. \end{aligned}$$

Therefore,

$$S_{m-3} = 2 \cdot \left((q^{\frac{1}{2}} + 8B_4 q^{\frac{3}{8}} i)^n + (q^{\frac{1}{2}} - 8B_4 q^{\frac{3}{8}} i)^n\right) \quad (18)$$

if $m = 4$, and

$$\begin{aligned} S_{m-3} = 2 \cdot & \left((-3q^{\frac{1}{2}} + \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} + 2^{m-1} B_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i)^n \right. \\ & \left. + (-3q^{\frac{1}{2}} + \sum_{r=3}^{m-3} 2^{r-1} A_r q^{\frac{2^{r-2}-1}{2^{r-1}}} - 2^{m-3} A_{m-2} q^{\frac{2^{m-4}-1}{2^{m-3}}} - 2^{m-1} B_m q^{\frac{2^{m-2}-1}{2^{m-1}}} i)^n \right) \end{aligned} \quad (19)$$

if $m \geq 5$. It is easy to check that S_2, \dots, S_{m-4} (for $m \geq 6$) and S_1 (for $m \geq 5$) are determined by (12) and (13), respectively. Moreover, if $m \geq 4$, then S_0 is determined by (14). For $m = 3$, we have

$$W_{1,0}(1) = -q^{1/2}, \quad W_{3,0}(1) = \pm 4|B_3|q^{1/4}i,$$

and so

$$S_0 = 2 \cdot \left((-q^{\frac{1}{2}} + 4B_3q^{\frac{1}{4}}i)^n + (-q^{\frac{1}{2}} - 4B_3q^{\frac{1}{4}}i)^n \right). \quad (20)$$

Substituting (12)–(20) into (5), we obtain the desired result. \square

4. THE CASE $p \equiv -3 \pmod{8}$

In this section, let $p \equiv -3 \pmod{8}$, $q = p^s \equiv 1 \pmod{2^m}$, $m \geq 2$. As in the previous sections, λ denotes a fixed character of order 2^m on \mathbb{F}_q .

For $r = 1, 2, \dots, m-1$, define the integers C_r and D_r by

$$p^{s/2^{r-1}} = C_r^2 + D_r^2, \quad C_r \equiv -1 \pmod{4}, \quad p \nmid C_r. \quad (21)$$

If $2^{m+1} \mid (q-1)$ (or, equivalently, $2^{m-1} \mid s$), we extend this notation to $r = m$. It is well known [4, Lemma 3.0.1] that for each fixed r , (21) determines C_r uniquely but determines D_r only up to sign. Further, if χ is a biquadratic character on $\mathbb{F}_{p^{s/2^{r-1}}}$ then $J(\chi) = C_r \pm |D_r|i$ (see [9, Proposition 2]). Appealing to Lemma 13, we obtain the following result.

Lemma 20. *Let r be an integer with $2^{r+1} \mid (q-1)$ and $2 \leq r \leq m$. Then*

$$G(\lambda^{2^{m-r}}) + G(\bar{\lambda}^{2^{m-r}}) = \begin{cases} 2C_r q^{(2^{r-1}-1)/2^r} & \text{if } 2^{r+2} \mid (q-1), \\ (-1)^{r-1} \cdot 2C_r q^{(2^{r-1}-1)/2^r} & \text{if } 2^{r+1} \parallel (q-1), \end{cases}$$

and

$$G(\lambda^{2^{m-r}}) - G(\bar{\lambda}^{2^{m-r}}) = \pm 2|D_r|q^{(2^{r-1}-1)/2^r}i.$$

To find $G(\lambda) \pm G(\bar{\lambda})$ in the case when $2^m \parallel (q-1)$, we need the next result.

Lemma 21. *Assume that $2^m \parallel (q-1)$. Then*

$$G(\lambda) + G(\bar{\lambda}) = \pm q^{(2^{m-1}-1)/2^m} i \sqrt{2(q^{1/2^{m-1}} - (-1)^m C_{m-1})}$$

and

$$G(\lambda) - G(\bar{\lambda}) = \pm q^{(2^{m-1}-1)/2^m} i \sqrt{2(q^{1/2^{m-1}} + (-1)^m C_{m-1})}.$$

Proof. By employing the same type of argument as in the proof of Lemma 17, we see that

$$\begin{aligned} (G(\lambda) + G(\bar{\lambda}))^2 &= -2q^{(2^{m-1}-1)/2^{m-1}} (q^{1/2^{m-1}} - (-1)^m C_{m-1}), \\ (G(\lambda) - G(\bar{\lambda}))^2 &= 2q^{(2^{m-1}-1)/2^{m-1}} (q^{1/2^{m-1}} + (-1)^m C_{m-1}). \end{aligned}$$

As $q^{1/2^{m-2}} = p^{s/2^{m-2}} = C_{m-1}^2 + D_{m-1}^2$, we have $q^{1/2^{m-1}} > |C_{m-1}|$, and the result follows. \square

We are now in a position to derive explicit formulas for N when $p \equiv -3 \pmod{8}$. We shall be using Lemmas 14, 20, 21 and Corollary 15 without mention.

Theorem 22. *Let $p \equiv -3 \pmod{8}$ and $2^{m+1} \mid (q-1)$. Then*

$$\begin{aligned} N &= q^{n-1} + \frac{q-1}{2^m q} \cdot \left[2^{m-2} \cdot \left((q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^n \right) \right. \\ &\quad + \sum_{t=1}^{m-2} 2^{m-t-2} \left((-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} + 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right. \\ &\quad \left. \left. + (-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} - 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right) \right. \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-1} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-1} C_m q^{\frac{2^{m-1}-1}{2^m}} \right)^n \\ &\quad \left. + \left(-q^{\frac{1}{2}} + \sum_{r=2}^m 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^n \right]. \end{aligned}$$

The integers C_r and $|D_r|$ are uniquely determined by (21).

Proof. We have

$$\begin{aligned} W_{1,m}(1) &= -q^{1/2}, \\ W_{r,m}(1) &= 2^{r-1} C_r q^{(2^{r-1}-1)/2^r}, \quad 2 \leq r \leq m-1, \quad m \geq 3, \\ W_{m,m}(1) &= \pm 2^{m-1} C_m q^{(2^{m-1}-1)/2^m}. \end{aligned}$$

Consequently,

$$\begin{aligned} S_{m-1} + S_m &= \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-1} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-1} C_m q^{\frac{2^{m-1}-1}{2^m}} \right)^n \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^m 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} \right)^n. \end{aligned} \tag{22}$$

Assume now that $1 \leq t \leq m-2$, $m \geq 3$. Then

$$\begin{aligned} W_{1,t}(1) &= -q^{1/2}, \\ W_{r,t}(1) &= 2^{r-1}C_r q^{(2^{r-1}-1)/2^r}, \quad 2 \leq r \leq t, \quad t \geq 2, \\ W_{t+1,t}(1) &= -2^t C_{t+1} q^{(2^t-1)/2^{t+1}}, \quad W_{t+2,t}(1) = \pm 2^{t+1} |D_{t+2}| q^{(2^{t+1}-1)/2^{t+2}}. \end{aligned}$$

Thus

$$\begin{aligned} S_t &= 2^{m-t-2} \left((-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} + 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right. \\ &\quad \left. + (-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} - 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right). \end{aligned} \quad (23)$$

Finally,

$$W_{1,0}(1) = q^{1/2}, \quad W_{2,0}(1) = \pm 2 |D_2| q^{1/4},$$

and so

$$S_0 = 2^{m-2} \cdot \left((q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^n \right). \quad (24)$$

Substituting (22)–(24) into (5), we obtain the assertion of the theorem. \square

Theorem 23. *Let $p \equiv -3 \pmod{8}$ and $2^m \parallel (q-1)$. If $m = 2$ then*

$$\begin{aligned} N &= q^{n-1} + \frac{q-1}{4q} \left[\left(-q^{\frac{1}{2}} + q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} + C_1)} \right)^n + \left(-q^{\frac{1}{2}} - q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} + C_1)} \right)^n \right. \\ &\quad \left. + \left(q^{\frac{1}{2}} + q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} - C_1)} \right)^n + \left(q^{\frac{1}{2}} - q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} - C_1)} \right)^n \right]. \end{aligned}$$

If $m \geq 3$ then

$$\begin{aligned} N &= q^{n-1} + \frac{q-1}{2^m q} \cdot \left[2^{m-2} \cdot \left((q^{\frac{1}{2}} + 2D_2 q^{\frac{1}{4}})^n + (q^{\frac{1}{2}} - 2D_2 q^{\frac{1}{4}})^n \right) \right. \\ &\quad + \sum_{t=1}^{m-3} 2^{m-t-2} \left((-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} + 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right. \\ &\quad \left. + (-q^{\frac{1}{2}} + \sum_{r=2}^t 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^t C_{t+1} q^{\frac{2^t-1}{2^{t+1}}} - 2^{t+1} D_{t+2} q^{\frac{2^{t+1}-1}{2^{t+2}}})^n \right) \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. + 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} - C_{m-1})} \right)^n \end{aligned}$$

$$\begin{aligned}
& + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. - 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}}-C_{m-1})} \right)^n \\
& + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. + 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}}+C_{m-1})} \right)^n \\
& + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. - 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}}+C_{m-1})} \right)^n \Big].
\end{aligned}$$

The integers C_r and $|D_r|$ are uniquely determined by (21).

Proof. Since $2^{m-2} \parallel s$, we conclude that

$$\begin{aligned}
W_{1,m}(1) &= \begin{cases} q^{1/2} & \text{if } m = 2, \\ -q^{1/2} & \text{if } m \geq 3, \end{cases} \\
W_{r,m}(1) &= 2^{r-1} C_r q^{(2^{r-1}-1)/2^r}, \quad 2 \leq r \leq m-2, \quad m \geq 4, \\
W_{m-1,m}(1) &= (-1)^m \cdot 2^{m-2} C_{m-1} q^{(2^{m-2}-1)/2^{m-1}}, \quad m \geq 3, \\
W_{m,m}(1) &= \pm 2^{m-2} q^{(2^{m-1}-1)/2^m} i \sqrt{2(q^{1/2^{m-1}} - (-1)^m C_{m-1})}.
\end{aligned}$$

Therefore,

$$S_{m-1} + S_m = \left(q^{\frac{1}{2}} + q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} - C_1)} \right)^n + \left(q^{\frac{1}{2}} - q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} - C_1)} \right)^n \quad (25)$$

if $m = 2$, and

$$\begin{aligned}
S_{m-1} + S_m &= \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. + 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} - (-1)^m C_{m-1})} \right)^n \\
& + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} + (-1)^m \cdot 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. - 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} - (-1)^m C_{m-1})} \right)^n \quad (26)
\end{aligned}$$

if $m \geq 3$. Further,

$$\begin{aligned} W_{1,m-2}(1) &= -q^{1/2}, \\ W_{r,m-2}(1) &= 2^{r-1}C_r q^{(2^{r-1}-1)/2^r}, \quad 2 \leq r \leq m-2, \quad m \geq 4, \\ W_{m-1,m-2}(1) &= -(-1)^m \cdot 2^{m-2}C_{m-1}q^{(2^{m-2}-1)/2^{m-1}}, \quad m \geq 3, \\ W_{m,m-2}(1) &= \pm 2^{m-2}q^{(2^{m-1}-1)/2^m} i \sqrt{2(q^{1/2^{m-1}} + (-1)^m C_{m-1})}. \end{aligned}$$

Hence

$$S_{m-2} = \left(-q^{\frac{1}{2}} + q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} + C_1)} \right)^n + \left(-q^{\frac{1}{2}} - q^{\frac{1}{4}} i \sqrt{2(q^{\frac{1}{2}} + C_1)} \right)^n \quad (27)$$

if $m = 2$, and

$$\begin{aligned} S_{m-2} &= \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1}C_r q^{\frac{2^{r-1}-1}{2^r}} - (-1)^m \cdot 2^{m-2}C_{m-1}q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. + 2^{m-2}q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} + (-1)^m C_{m-1})} \right)^n \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1}C_r q^{\frac{2^{r-1}-1}{2^r}} - (-1)^m \cdot 2^{m-2}C_{m-1}q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. - 2^{m-2}q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} + (-1)^m C_{m-1})} \right)^n \end{aligned} \quad (28)$$

if $m \geq 3$. By combining (26) and (28) and examining the two cases m odd and m even separately, we infer that for $m \geq 3$,

$$\begin{aligned} S_{m-2} + S_{m-1} + S_m &= \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1}C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-2}C_{m-1}q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. + 2^{m-2}q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} - C_{m-1})} \right)^n \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1}C_r q^{\frac{2^{r-1}-1}{2^r}} + 2^{m-2}C_{m-1}q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. - 2^{m-2}q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} - C_{m-1})} \right)^n \\ &\quad + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1}C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2}C_{m-1}q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\ &\quad \left. + 2^{m-2}q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} + C_{m-1})} \right)^n \end{aligned}$$

TABLE 1. Numerical results.

p	s	m	n	N	p	s	m	n	N
3	4	3	3	7041	5	2	2	5	498625
3	4	3	4	1130241	5	2	3	4	12289
3	4	3	5	41304321	5	2	3	5	129025
3	4	4	3	20481	5	4	2	3	416833
3	4	4	4	81921	5	4	2	4	250892929
3	4	4	5	126033921	5	4	3	3	94849
3	8	3	3	30805761	5	4	3	4	304182529
3	8	4	3	42298881	5	4	4	3	319489
3	8	5	3	167936001	5	4	4	4	369328129

$$\begin{aligned}
& + \left(-q^{\frac{1}{2}} + \sum_{r=2}^{m-2} 2^{r-1} C_r q^{\frac{2^{r-1}-1}{2^r}} - 2^{m-2} C_{m-1} q^{\frac{2^{m-2}-1}{2^{m-1}}} \right. \\
& \quad \left. - 2^{m-2} q^{\frac{2^{m-1}-1}{2^m}} i \sqrt{2(q^{\frac{1}{2^{m-1}}} + C_{m-1})} \right)^n. \quad (29)
\end{aligned}$$

It is readily seen that for $m \geq 3$ the sums S_0, \dots, S_{m-3} are determined by (23) and (24). Substituting (23), (24), (25), (27), (29) into (5), we deduce the desired result. \square

5. NUMERICAL RESULTS

The theoretical results of this paper are supported by numerical experiments. Some numerical results are listed in Table 1.

6. CONCLUDING REMARKS

The results of the previous sections can be applied to some other diagonal equations. As before, $2^m \mid (q-1)$, $N = N[x_1^{2^m} + \dots + x_n^{2^m} = 0]$ and λ denotes a character of order 2^m on \mathbb{F}_q .

Granville, Li and Sun [7] have shown that

$$N[a_1 x_1^{d_1} + \dots + a_n x_n^{d_n} = 0] = N[a_1 x_1^{w_1} + \dots + a_n x_n^{w_n} = 0],$$

where $w_j = \gcd(d_j, \text{lcm}(d_1, \dots, d_{j-1}, d_{j+1}, \dots, d_n))$, $1 \leq j \leq n$. Thus, if h_1, \dots, h_n are pairwise coprime positive integers with $2^m h_1 \dots h_n \mid (q-1)$, then

$$N[x_1^{2^m h_1} + \dots + x_n^{2^m h_n} = 0] = N[x_1^{2^m} + \dots + x_n^{2^m} = 0] = N,$$

and so our formulas are valid for some more general equations.

Let $u_1 > 2, \dots, u_t > 2$ be pairwise coprime odd positive integers with $u_j \mid (q-1)$ for all j . Assume in addition that for each $j \in \{1, \dots, t\}$ there exists a positive integer ℓ_j such that $u_j \mid (p^{\ell_j} + 1)$, with ℓ_j chosen minimal. It follows from [4, Theorem 11.6.2] that $2\ell_j \mid s$ for all j . Cao and Sun [6] obtained the factorization

formulas for the number of solutions to diagonal equations. Combining their result with [15, Corollary 4], we infer that

$$\begin{aligned} N[x_1^{2^m} + \cdots + x_n^{2^m} + y_{11}^{u_1} + \cdots + y_{1n_1}^{u_1} + \cdots + y_{t1}^{u_t} + \cdots + y_{tn_t}^{u_t} = 0] \\ = q^{n+n_1+\cdots+n_t-1} + (-1)^{\sum_{j=1}^t ((s/\ell_j)-1)n_j} (N - q^{n-1}) q^{(n_1+\cdots+n_t)/2} \\ \times \prod_{j=1}^t \frac{(u_j - 1)^{n_j} + (-1)^{n_j} (u_j - 1)}{u_j}. \end{aligned}$$

Now let $k \geq 2$ be even and $b_1, \dots, b_k \in \mathbb{F}_q^*$. Lemma 1 yields

$$\begin{aligned} N[x_1^{2^m} + \cdots + x_n^{2^m} + b_1 y_1^2 + \cdots + b_k y_k^2 = 0] \\ = q^{n+k-1} + \frac{q-1}{q} \sum_{\substack{1 \leq j_1, \dots, j_n \leq 2^m-1 \\ j_1 + \cdots + j_n \equiv 0 \pmod{2^m}}} \eta(b_1 \cdots b_k) G(\eta)^k G(\lambda^{j_1}) \cdots G(\lambda^{j_n}). \end{aligned}$$

Since, by Lemma 2(a), $G(\eta)^2 = \eta(-1)q$, we deduce that

$$N[x_1^{2^m} + \cdots + x_n^{2^m} + b_1 y_1^2 + \cdots + b_k y_k^2 = 0] = q^{n+k-1} + \eta((-1)^{k/2} b_1 \cdots b_k) q^{k/2} (N - q^{n-1}).$$

In particular,

$$\begin{aligned} N[x_1^{2^m} + x_2^{2^m} + b_1 y_1^2 + \cdots + b_k y_k^2 = 0] \\ = q^{k+1} + \eta((-1)^{k/2} b_1 \cdots b_k) q^{k/2} (q-1) \cdot \begin{cases} 2^m - 1 & \text{if } 2^{m+1} \mid (q-1), \\ -1 & \text{if } 2^m \parallel (q-1), \end{cases} \end{aligned}$$

which is a special case of a result of Sun [12].

Finally, we notice that in the more general case where f is a nondegenerate quadratic form over \mathbb{F}_q in an even number k of variables, we have

$$N[x_1^{2^m} + \cdots + x_n^{2^m} + f(y_1, \dots, y_k) = 0] = q^{n+k-1} + \eta((-1)^{k/2} \Delta) q^{k/2} (N - q^{n-1}),$$

where Δ denotes the determinant of f .

ACKNOWLEDGMENT

The author thanks the referee for a careful reading of the manuscript and helpful suggestions.

REFERENCES

- [1] I. Baoulina, Generalizations of the Markoff-Hurwitz equations over finite fields, *J. Number Theory* **118** (2006) 31–52.
- [2] I. Baoulina, On the number of solutions to the equation $(x_1 + \cdots + x_n)^2 = ax_1 \cdots x_n$ in a finite field, *Int. J. Number Theory* **4** (2008) 797–817.
- [3] I. Baoulina, On the number of solutions to certain diagonal equations over finite fields, *Int. J. Number Theory* **6** (2010) 1–14.
- [4] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley-Interscience, New York, 1998).
- [5] R. F. Beyl, Cyclic subgroups of the prime residue group, *Am. Math. Mon.* **84** (1977) 46–48.

- [6] W. Cao and Q. Sun, Factorization formulae on counting zeros of diagonal equations over finite fields, *Proc. Am. Math. Soc.* **135** (2007) 1283–1291.
- [7] A. Granville, S. Li and Q. Sun, On the number of solutions of the equation $\sum_{i=1}^n x_i/d_i \equiv 0 \pmod{1}$ and of diagonal equations in finite fields, *Sichuan Daxue Xuebao* **32** (1995) 243–248.
- [8] J. R. Joly, Nombre de solutions de certaines équations diagonales sur un corps fini, *C. R. Acad. Sci. Paris Ser. A–B* **272** (1971) 1549–1552.
- [9] S. A. Katre and A. R. Rajwade, Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum, *Math. Scand.* **60** (1987) 52–62.
- [10] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, MA, 1983).
- [11] G. L. Mullen and D. Panario, *Handbook of Finite Fields* (CRC Press, 2013).
- [12] Q. Sun, On diagonal equations over finite fields, *Finite Fields Appl.* **3** (1997) 175–179.
- [13] Q. Sun and P.-Z. Yuan, On the number of solutions of diagonal equations over a finite field, *Finite Fields Appl.* **2** (1996) 35–41.
- [14] A. Weil, Numbers of solutions of equations in finite fields, *Bull. Am. Math. Soc.* **55** (1949) 497–508.
- [15] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory* **42** (1992) 247–257.
- [16] J. Wolfmann, New results on diagonal equations over finite fields from cyclic codes, *Contemp. Math.* **168** (1994) 387–395.

DEPARTMENT OF MATHEMATICS, MOSCOW STATE PEDAGOGICAL UNIVERSITY, KRASNO-PRUDNAYA STR. 14, MOSCOW 107140, RUSSIA

E-mail address: jbaulina@mail.ru